REMARKS

Claims 2-4, 10-12, 16, 17, 20-22, 26, 27, 30-32, 36 and 37 are pending in the present application. No claims were amended, cancelled or added. Reconsideration of the claims is respectfully requested.

I. 35 U.S.C. § 102, Anticipation, Claims 2-4, 10, 20, and 30

The Examiner has rejected claims 10, 20 and 30 under 35 U.S.C. § 102(b) as being anticipated by US 5,991,881, to Conklin et al. This rejection is respectfully traversed. In the Office Action, the Examiner stated the following in reference to claims 10, 20 and 30:

> Claims 10,20,30: Conklin disclose receiving at a bait server a request to perform a function on the bait server and identifying an offending system which the request originated in (col.6,lines 10-19). Conklin disclose alerting a local server that a virus is in progress and of the identity of the offending system and disconnecting the offending system from the network in (col. 6,lines 34-43; col.7 55-61).

Office Action dated June 22, 2005, page 2

A prior art reference anticipates the claimed invention under 35 U.S.C. § 102 only if every element of a claimed invention is identically shown in that single reference, arranged as they are in the claims. *In re Bond*, 910 F.2d 831, 832, 15 U.S.P.Q.2d 1566, 1567 (Fed. Cir. 1990). All limitations of the claimed invention must be considered when determining patentability. *In re Lowry*, 32 F.3d 1579, 1582, 32 U.S.P.Q.2d 1031, 1034 (Fed. Cir. 1994). Anticipation focuses on whether a claim reads on the product or process a prior art reference discloses, not on what the reference broadly teaches. *Kalman v. Kimberly-Clark Corp.*, 713 F.2d 760, 218 U.S.P.Q. 781 (Fed. Cir. 1983). The Conklin reference cited by the Examiner does not anticipate the present invention as recited in claim 10, because Conklin fails to teach each and every element of claim 10. Independent claim 10, which is representative of independent claims 20 and 30 with regards to similarly recited subject matter, reads as follows:

> 10. A method for detecting the presence of a computer virus, the method comprising;
>
> receiving, at a bait server, a request to perform a function on the bait server;

identifying an offending system from which the request originated;
alerting a local server that a virus attack is in progress and of the identity of the offending system; and
disconnecting the offending system from the network.

Conklin does not teach each and every feature of the presently claimed invention in claim 10. Claim 10 recites the feature of "receiving, at a bait server, a request to perform a function on the bait server." Conklin does not teach this feature. The Examiner points to column 6, lines 10 through 19, reproduced below for the Examiner's convenience, as teaching this feature:

> Responses to an attack include a description of the identified event with the attacking network address, targeted network address and a date/time stamp. This information is sent to the local system console by default but can be configured to send to any number of remote SNMP monitoring systems. The system can also be configured to transmit all message data contained within the Trap PDU in encrypted (using the Data Encryption Standard--DES in the preferred embodiment) format to the remote monitoring systems.

The above cited passage does not teach the feature of "receiving, at a bait server, a request to perform a function on the bait server." Instead, the above cited passage teaches that in response to an attack a message is sent to either a local system or a remote SNMP monitoring system. The passage also explains that the information to be sent can be encrypted. The message is sent as a Trap PDU. The term Trap PDU is a well known term in the art and refers to a type of data packet, an IEEE standard SNMP data packet, as Conklin explains in a passage in column 5, lines 46 through 61, reproduced below for the Examiner's convenience:

> This Function is the first in a sequence of events which occur immediately following detection of reportable activity indicating an unauthorized event or series of events indicating an unauthorized activity on a network segment. Characteristics of the reportable activity such as an attempted intrusion, which may be called an attack, are encapsulated into an alarm message called a Send Alert message which is also date/time stamped. In the preferred embodiment, the Send Alert Message is formatted into data structures, updates the stand-alone system console, or is transmitted using IEEE standard Simple Network Management Protocol (SNMP) data packets referred to as Trap PDUs (protocol data units in the preferred embodiment) to a network management system, depending on current Network Surveillance System system configuration.

(emphasis added)

Conklin further defines what the term Trap PDU means in column 5, line 63, through column 6, line 9, reproduced below for the Examiner's convenience:

> A Trap PDU is issued by an SNMP enabled software application. It is used to provide the remote SNMP-based network management station with an asynchronous notification of some significant event. The following is the field definition of a Trap PDU:
> PDU type: indicates a GetRequest PDU,
> enterprise: identifies the system that generated the trap,
> agent-address: IP address of the object generating the trap,
> generic-trap: one of the predefined trap types,
> specific-trap: a code that indicates more specifically the nature of the trap,
> time-stamp: time of the generation of the trap, and
> variable-bindings: implementation specific information relating to the trap.

As can be seen from the above cited passages, a Trap PDU is a format of data packets which contains specific information about the attack that has been detected by the surveillance system. Therefore, the above cited passage of Conklin, column 6, lines 10 through 19, does not teach the feature of "receiving, at a bait server, a request to perform a function on the bait server," as neither the cited passage, nor does any passage of Conklin teach a bait server. Thus, Conklin does not teach the feature of "receiving, at a bait server, a request to perform a function on the bait server," as recited in claim 10 of the present invention. Therefore Conklin does not anticipate the present invention as recited in claim 10, because Conklin fails to teach each and every element of claim 10.

Therefore, for all the reasons set forth above, Applicants submit that independent claims 10, 20, and 30 are not taught by Conklin. Accordingly, Applicants respectfully submit that claims 10, 20, and 30 are patentable over the Conklin reference.

Claims 2-4 are dependent claims depending from independent claims 10, 20, and 30, respectively. As Applicants have already demonstrated that independent claims 10, 20, and 30 are patentable over the Conklin reference, Applicants submit that dependent claims 2-4 are patentable over the Conklin reference at least by virtue of depending from an allowable claim. Additionally, claims 2-4 claim other additional combinations of features not suggested by the reference.

For example, claim 2, which is representative of claims 3 and 4 with regard to similarly recited subject matter, recites the feature of "not publishing the bait server's address to the network." This feature is not taught or suggested by Conklin. As was discussed above with regards to claim 10, Conklin does not teach a bait server, therefore Conklin cannot teach the feature of "not publishing the bait server's address to the network." The Examiner points to column 1, lines 66 through 67, reproduced below for the Examiner's convenience, of Conklin as teaching this feature:

> This System is transparent to the intruder, as it has no discernible address.

The above cited passage does not teach the feature of "not publishing the bait server's address to the network." Instead, the above cited passage of Conklin teaches that the monitoring system has no discernable address and therefore appears transparent to the intruder. The passage makes no mention of the actual network or of "not publishing the bait server's address to the network." However, this transparency is more fully explained in column 3, line 44 though line 60, reproduced below for the Examiner's convenience:

> The Network Surveillance System operates through a computer, attached to the network, in the preferred embodiment by an interface card, as shown in **FIG. 5**. In the preferred embodiment, as shown in **FIG. 4**, the network interface card contains a preset and unique identifier known as an Ethernet address or hardware address. The unique address, provides the means for an attached computer system to identify intended packets and ignore the rest, as is well known in the art. The Network Surveillance System utilizes standard device drivers to forward all packets into the host from the network regardless of the address in the packets. This is generally known in a UNIX-based operating system as running in "promiscuous mode," as is well known in the art.
>
> This promiscuous mode makes the System transparent and inaccessible to an intruder and preserves the authenticity of the logged entries mode by the System.

The above cited passage teaches that the monitoring system as taught by Conklin is transparent because its network card functions in "promiscuous mode," which is well known in the art. Promiscuous mode refers to the practice of putting a network card into a setting so that it passes all traffic it receives to the CPU rather than just packets addressed to it. Therefore, the address of the network card does not go unpublished. Rather, the address of the network card is published to the network, but the network card captures all information bound for any address, not just for its own address. Therefore, Conklin does not teach the feature of "not publishing the bait server's address to the network," as recited in claim 2 of the present invention.

Therefore, for all the reasons set forth above, Applicants submit that Conklin does not anticipate claims 2-4 of the present invention, as Conklin fails to teach each and every element of claims 2-4. Accordingly, Applicants respectfully submit that claims 2-4 are patentable over the Conklin reference in their own right as well as by virtue of their depending from an allowable claim.

Therefore, the rejection of claims 2-4, 10, 20, and 30 under 35 U.S.C. § 102 has been overcome.

Furthermore, Conklin does not teach, suggest, or give any incentive to make the needed changes to reach the presently claimed invention. Conklin actually teaches away from the presently claimed invention because it teaches a system for monitoring activity on a network to detect when the network has been attacked and which <u>cannot be accessed by a hacker or intruder</u> (see Conklin, col. 1, line 66 – col. 2, line 4; col. 3, lines 58-60), as opposed to a bait server which is attacked instead of the network, as in the presently claimed invention. Absent the Examiner pointing out some teaching or incentive to implement Conklin and a bait server which is attacked instead of the network, one of ordinary skill in the art would not be led to modify Conklin to reach the present invention when the reference is examined as a whole. Absent some teaching, suggestion, or incentive to modify Conklin in this manner, the presently claimed invention can be reached only through an improper use of hindsight using the Applicants' disclosure as a template to make the necessary changes to reach the claimed invention.

II. <u>35 U.S.C. § 103, Obviousness, claims 11-12, 16, 21, 22, 26-27, 31, 32 and 36-37</u>

The Examiner has rejected claims 11-12, 16, 21, 22, 26-27, 31, 32 and 36-37 under 35 U.S.C. § 103(a) as being unpatentable over US 5,991,981, to Conklin et al. This rejection is respectfully traversed.

In the Office Action, in reference to claims 16, 26 and 36, the Examiner stated the following:

> Claims 16,26, 36: Conklin disclose receiving at a bait server a request to perform a function on the bait server and identifying an offending system which the request originated in (col.6,lines 10-19). Conklin disclose publishing the bait server's address to the network in (col.1,lines 66-7). Conklin disclose alerting a local server that a virus is in progress and of the identity of the offending system and disconnecting the offending system from the network in (col.6, lines 34-43;col.7,lines 55-61). Conklin does not specifically disclose prior to disconnecting the offending system, notifying the offending system that it is infected with a virus. It would have been obvious to person of ordinary skill in the art to modify the invention of Conklin to prior to disconnecting the offending system, notifying the offending system that it is infected with a virus in order to prevent virus from spreading system to system so that offending system can be disinfected before reconnecting to the network thus allowing network to run virus free. Further, directing all devices to ignore a communication requests from offending system would have been obvious in order to stop any virus from entering the network.

Office Action dated June 22, 2005, page 3

Claims 16, 26, and 36 are independent claims which recite features to be performed by a bait server. As was discussed above regarding the rejection of claim 10, Conklin does not teach the use of a bait server. Claims 11, 12, 17, 21, 22, 27, 31, 32, and 37 are dependent claims depending from independent claims 10, 16, 20, 26, 30, and 36. Therefore, the Conklin reference still does not teach or suggest all the claim limitations in claims 11-12, 16, 21, 22, 26-27, 31, 32 and 36-37, as argued in response to the rejection of claim 10 above.

Furthermore, the Examiner's assertions do not cure the deficiencies of Conklin. The Examiner's assertions do not teach the features missing from Conklin, including "a bait server," "receiving, at a bait server, a request to perform a function on the bait server," or "not publishing the bait server's address to a network." Additionally, claims 11, 12, 17, 21, 22, 27, 31, 32, and 37 recite additional features not found in Conklin. The Examiner has alleged that all of these additional features are obvious. However, the Examiner has failed to explain why it would be obvious to modify Conklin to reach the presently claimed invention.

The Examiner bears the burden of establishing a *prima facie* case of obviousness based on the prior art when rejecting claims under 35 U.S.C. § 103. *In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992). In addition, the Examiner may not make modifications to the prior art using the claimed invention as a model for the modifications. *In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q.2d 1780, 1783-1784 (Fed. Cir. 1992). "The mere fact that the prior art may be modified in the manner suggested by the Examiner does not make the modification obvious unless the prior art has suggested the desirability of the modification." *Id.* In other words, unless some teaching exists in the prior art for the suggested modification, merely asserting that such a modification would be obvious to one of ordinary skill in the art is improper and cannot be used to meet the burden of establishing a *prima facie* case of obviousness. Such reliance is an impermissible use of hindsight with the benefit of Applicants' disclosure.

Therefore, absent some teaching, suggestion, or incentive in the prior art, Conklin cannot be properly modified to form the claimed invention. As a result, absent any teaching, suggestion, or incentive from the prior art to make the proposed modifications, the presently claimed invention can be reached only through an impermissible use of hindsight with the benefit of Applicants' invention as a model.

Furthermore, Conklin actually teaches away from the presently claimed invention since Conklin teaches a third party monitoring system which <u>cannot be accessed by a hacker or intruder</u> (see Conklin, col. 1, line 66 – col. 2, line 4; col. 3, lines 58-60), as opposed to a bait server which is attacked instead of the network, as in the presently claimed invention. *See In re Hedges*, 228 U.S.P.Q. 685 (Fed. Cir. 1986). Thus, one of ordinary skill in the art would not be motivated to make the changes proposed by the Examiner.

"It is impermissible within the framework of section 103 to pick and choose from any one reference only so much of it as will support a given position, to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one of ordinary skill in the art." *In re Hedges*, 228 U.S.P.Q. at 687. Thus, when Conklin is examined as a whole, Conklin teaches one of ordinary skill in the art, which teaches away from a bait server which is attacked instead of the network, as in the presently claimed invention. Therefore, one of ordinary skill in the art would not be motivated to make the Examiner's proposed changes.

Therefore, the rejection of claims 11-12, 16, 21, 22, 26-27, 31, 32 and 36-37 under 35 U.S.C. § 103 has been overcome.

III. Conclusion

It is respectfully urged that the subject application is patentable over Conklin et al. (US 5,991,881) and is now in condition for allowance.

The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: September 14, 2005

Respectfully submitted,

Gerald H. Glanzman
Reg. No. 25,035
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Attorney for Applicants

GHG/bj